

# OPIS PRZEDMIOTU ZAMÓWIENIA

w postępowaniu o udzielenie zamówienia publicznego w trybie podstawowym bez negocjacji o wartości zamówienia mniejszej niż kwoty określone w obwieszczeniu Prezesa Urzędu Zamówień Publicznych, ogłoszonym na podstawie art. 3 ust. 3 ustawy z dnia 11 września 2019 r. Prawo zamówień publicznych (Dz.U. 2024 poz. 1320 ze zm.), pod nazwą:

## Dostawa sprzętu informatycznego do zapewnienia bezpieczeństwa sieci – urządzenia UTM

Część 1 zamówienia na „Dostawę sprzętu informatycznego” będącego częścią projektu pn. „Cyberbezpieczna Gmina Porąbka”

**Zamawiający:** Gmina Porąbka, ul. Krakowska 3, 43-353 Porąbka

Projekt finansowany ze środków Funduszy Europejskich na Rozwój Cyfrowy (FERC) 2021-2027 Priorytet II „Zaawansowane usługi cyfrowe” Działanie 2.2 „Wzmocnienie krajowego systemu cyberbezpieczeństwa”

L.P.	WYMAGANE MINIMALNE PARAMETRY JAKOŚCIOWE	PARAMETR WYMAGANY / POŻĄDANY	PUNKTACJA	PARAMETR OFEROWANY – WYKONAWCA WINIEN OPISAĆ/PODAĆ OFEROWANE PARAMETRY	
I.	Rozbudowa zapory sieciowej UTM				
1	INFORMACJE OGÓLNE				
1)	Producent/Nazwa rozwiązania/Model	WYMAGANY	NIE DOTYCZY	DT	Podać producenta, nazwę oraz model
2)	Zamawiający obecnie używa zapory sieciowej UTM Fortigate 80f. W ramach rozbudowy należy dostarczyć kompatybilne urządzenie umożliwiające utworzenie klastra HA wraz z zapewnieniem jednolitej gwarancji na całość rozwiązania.	WYMAGANY	NIE DOTYCZY		Nie dotyczy
3)	Zamawiający dopuszcza rozwiązanie równoważne, w którym każde urządzenie musi spełniać minimalne wymagania parametrach zgodnie z pkt. 2 – pkt 18. Zamawiający zastrzega, że w przypadku oferowania rozwiązania równoważnego należy uwzględnić wdrożenie systemu, wraz z przeniesieniem całej konfiguracji i odzwierciedlenie usług na nowym rozwiązaniu – bez przerwy w dostępie do usług po stronie Zamawiającego i poza godzinami pracy urzędu.	WYMAGANY	NIE DOTYCZY		Nie dotyczy
2	WYMAGANIA OGÓLNE				
1)	Rozwiązanie musi być dostarczone w postaci komercyjnej platformy sprzętowej z zabezpieczonym systemem operacyjnym.	WYMAGANY	NIE DOTYCZY		Opisać oferowane parametry
2)	Musi być wyposażone w moduł TPM	WYMAGANY	NIE DOTYCZY		Opisać oferowane parametry
3)	Rozwiązanie musi umożliwiać utworzenie klastra wysokiej dostępności HA co najmniej w trybie Active-Pasive	WYMAGANY	NIE DOTYCZY		Opisać oferowane parametry
4)	Komunikacja klastra wysokiej dostępności musi być tworzona za pomocą redundantnych połączeń światłowodowych i odbywać się poprzez dwa interfejsy SFP	WYMAGANY	NIE DOTYCZY		Opisać oferowane parametry



Fundusze Europejskie  
na Rozwój Cyfrowy



Rzeczpospolita  
Polska

Dofinansowane przez  
Unię Europejską



CENTRUM  
PROJEKTÓW  
POLSKA  
CYFROWA

5)	System musi wspierać protokół LACP (Link Aggregation Control Protocol) zgodny z normą IEEE 802.3ad.	WYMAGANY	NIE DOTYCZY		Opisać oferowane parametry
<b>3 INTERFEJSY</b>					
1)	minimum 6 interfejsów 1 GbE RJ45	WYMAGANY	NIE DOTYCZY		Opisać oferowane parametry
2)	minimum 2 interfejsy 1 GbE SFP	WYMAGANY	NIE DOTYCZY		Opisać oferowane parametry
3)	Możliwość tworzenia minimum 128 interfejsów wirtualnych definiowanych jako VLANy w oparciu o standard 802.1q.	WYMAGANY	NIE DOTYCZY		Opisać oferowane parametry
<b>4 PAMIĘĆ</b>					
1)	Dysk SSD o pojemności minimum 64GB	WYMAGANY	NIE DOTYCZY		Opisać oferowane parametry
<b>5 ZASILANIE</b>					
1)	Redundantny zasilacz o mocy dopasowanej do samodzielnego zapewnienia zasilania urządzenia, pracujące w sieci 230V 50/60Hz.	WYMAGANY	NIE DOTYCZY		Opisać oferowane parametry
<b>6 FUNKCJE BEZPIECZEŃSTWA</b>					
1)	<p>System ochrony musi realizować wszystkie z poniższych funkcjonalności. Poszczególne funkcjonalności systemu bezpieczeństwa mogą być realizowane w postaci osobnych platform sprzętowych lub programowych:</p> <ul style="list-style-type: none"> <li>– kontrola dostępu – zaporą ogniową klasy Stateful Inspection</li> <li>– kontrola stron Internetowych – Web Filter [WF]</li> <li>– kontrola zawartości poczty – antyspam [AS] (dla protokołów SMTP, POP3)</li> <li>– kontrola pasma oraz ruchu [QoS i Traffic shaping]</li> <li>– kontrola aplikacji oraz rozpoznawanie ruchu P2P</li> <li>– ochrona przed wirusami – antywirus [AV] (dla protokołów SMTP, POP3, HTTP, FTP, HTTPS). Skanowanie AV dla plików typu: rar, zip;</li> <li>– ochrona przed atakami - Intrusion Prevention System [IPS/IDS]</li> </ul>	WYMAGANY	NIE DOTYCZY		Opisać oferowane parametry



	– poufność danych - IPSec VPN oraz SSL VPN analiza ruchu szyfrowanego protokołem SSL				
<b>7</b>	<b>FIREWALL</b>				
1)	Urządzenie ma być wyposażone w Firewall klasy Stateful Inspection.	WYMAGANY	NIE DOTYCZY		Opisać oferowane parametry
2)	Obsługa translacji NAT oraz PAT.	WYMAGANY	NIE DOTYCZY		Opisać oferowane parametry
3)	Ochrona przed atakami DoS oraz DDoS (flood protection).	WYMAGANY	NIE DOTYCZY		Opisać oferowane parametry
4)	Ochrona przed skanowaniem portów.	WYMAGANY	NIE DOTYCZY		Opisać oferowane parametry
5)	Blokowanie ruchu na podstawie kraju pochodzenia (geolokalizacja IP).	WYMAGANY	NIE DOTYCZY		Opisać oferowane parametry
6)	Filtrowanie na poziomie warstwy 2 modelu OSI tj. na podstawie adresów MAC.	WYMAGANY	NIE DOTYCZY		Opisać oferowane parametry
7)	Możliwość ustawienia trybu pracy jako router warstwy trzeciej, jako bridge warstwy drugiej oraz hybrydowo (częściowo jako router, a częściowo jako bridge).	WYMAGANY	NIE DOTYCZY		Opisać oferowane parametry
8)	Możliwość uwierzytelnienia i autoryzacji użytkowników w oparciu o bazę LDAP, zewnętrzny serwer RADIUS, zewnętrzny serwer Kerberos.	WYMAGANY	NIE DOTYCZY		Opisać oferowane parametry
9)	Musi posiadać wbudowany posiadać wbudowany analizator reguł, który wskazuje błędy i sprzeczności w konfiguracji reguł.	WYMAGANY	NIE DOTYCZY		Opisać oferowane parametry
10)	Możliwość tworzenia wydzielonych stref bezpieczeństwa Firewall np. DMZ.	WYMAGANY	NIE DOTYCZY		Opisać oferowane parametry
<b>8</b>	<b>VPN</b>				
1)	Tworzenie połączeń w topologii Site-to-site oraz możliwość definiowania połączeń Client-to-site.	WYMAGANY	NIE DOTYCZY		Opisać oferowane parametry
2)	Wsparcie sieci VPN typu, minimum: PPTP VPN, IPSec VPN, SSL VPN	WYMAGANY	NIE DOTYCZY		Opisać oferowane parametry
3)	Klient VPN producenta rozwiązania współpracujący z dostarczonym rozwiązaniem.	WYMAGANY	NIE DOTYCZY		Opisać oferowane parametry
4)	Monitorowanie stanu tuneli VPN i stałego utrzymywania ich aktywności.	WYMAGANY	NIE DOTYCZY		Opisać oferowane parametry
5)	Możliwość przełączania tunelu na łącze zapasowe na wypadek awarii łącza dostawcy podstawowego (VPN Failover)	WYMAGANY	NIE DOTYCZY		Opisać oferowane parametry

6)	Praca w topologii Hub and Spoke oraz Mesh lub równoważnej.	WYMAGANY	NIE DOTYCZY		<i>Opisać oferowane parametry</i>
7)	Obsługa mechanizmów minimum IPSec NAT Traversal, DPD, Xauth.	WYMAGANY	NIE DOTYCZY		<i>Opisać oferowane parametry</i>
8)	Obsługa SSL VPN w trybach portal oraz tunel.	WYMAGANY	NIE DOTYCZY		<i>Opisać oferowane parametry</i>
<b>9</b>	<b>IPS</b>				
1)	Wykrywanie włamań oraz anomalii w ruchu sieciowym przy pomocy analizy protokołów, analizy heurystycznej oraz analizy w oparciu o sygnatury kontekstowe.	WYMAGANY	NIE DOTYCZY		<i>Opisać oferowane parametry</i>
2)	Usuwanie szkodliwej zawartości w kodzie HTML oraz JavaScript żądanej przez użytkownika strony internetowej bez blokowania dostępu do tej strony po usunięciu zagrożenia	WYMAGANY	NIE DOTYCZY		<i>Opisać oferowane parametry</i>
3)	Baza wykrywanych ataków musi zawierać co najmniej 1000 wpisów.	WYMAGANY	NIE DOTYCZY		<i>Opisać oferowane parametry</i>
4)	Wykrywanie anomalii protokołów i ruchu stanowiących podstawową ochronę przed atakami typu DoS oraz DDoS.	WYMAGANY	NIE DOTYCZY		<i>Opisać oferowane parametry</i>
<b>10</b>	<b>ANTYWIRUS</b>				
1)	Silnik antywirusowy musi zapewniać skanowanie ruchu w obu kierunkach komunikacji dla protokołów działających na niestandardowych portach (np. FTP na porcie 2021).	WYMAGANY	NIE DOTYCZY		<i>Opisać oferowane parametry</i>
2)	Możliwość pracy w trybie przezroczystego serwera poczty (Transparent Email Proxy)	WYMAGANY	NIE DOTYCZY		<i>Opisać oferowane parametry</i>
3)	Automatyczna aktualizacja sygnatur zagrożeń.	WYMAGANY	NIE DOTYCZY		<i>Opisać oferowane parametry</i>
4)	Ochrona przed spamem i szkodliwym oprogramowaniem w trakcie transakcji SMTP.	WYMAGANY	NIE DOTYCZY		<i>Opisać oferowane parametry</i>
5)	Inspekcja komunikacji email realizowanej przy użyciu protokołów SMTP, SMTPS, POP3, POP3S.	WYMAGANY	NIE DOTYCZY		<i>Opisać oferowane parametry</i>

6)	Wykrywanie, blokowanie i skanowanie załączników poczty email.	WYMAGANY	NIE DOTYCZY		Opisać oferowane parametry
7)	Tworzenie białych i czarnych list adresów email.	WYMAGANY	NIE DOTYCZY		Opisać oferowane parametry
8)	Wykrywanie spamu niezależnie od stosowanego języka.	WYMAGANY	NIE DOTYCZY		Opisać oferowane parametry
9)	Musi korzystać minimum z dwóch różnych serwerów publikujących listy RBL.	WYMAGANY	NIE DOTYCZY		Opisać oferowane parametry
<b>11 KONTROLA APLIKACJI</b>					
1)	Kontrola ruchu na podstawie głębokiej analizy pakietów, nie bazującej jedynie na wartościach portów TCP/UDP.	WYMAGANY	NIE DOTYCZY		Opisać oferowane parametry
2)	Wykrywanie i kontrolę mikroaplikacji (np. Gry portalu Facebook).	WYMAGANY	NIE DOTYCZY		Opisać oferowane parametry
3)	Identyfikacja aplikacji niezależnie od wykorzystywanego portu, protokołu, szyfrowania.	WYMAGANY	NIE DOTYCZY		Opisać oferowane parametry
<b>12 FILTR STRON WWW</b>					
1)	Wbudowany filtr URL.	WYMAGANY	NIE DOTYCZY		Opisać oferowane parametry
2)	Musi udostępniać kategorie minimum spam, hacking, malware, botnets.	WYMAGANY	NIE DOTYCZY		Opisać oferowane parametry
3)	Baza filtra WWW musi umożliwiać grupowanie w kategorie tematyczne.	WYMAGANY	NIE DOTYCZY		Opisać oferowane parametry
4)	Filtrowanie treści oraz szkodliwego oprogramowania w obrębie protokołów HTTP i HTTPS.	WYMAGANY	NIE DOTYCZY		Opisać oferowane parametry
5)	Możliwość blokowania i wysyłania treści poprzez HTTP i HTTPS.	WYMAGANY	NIE DOTYCZY		Opisać oferowane parametry
6)	Inspekcja z obsługą protokołu TLS 1.3.	WYMAGANY	NIE DOTYCZY		Opisać oferowane parametry
7)	Filtrowanie plików na podstawie MIME.	WYMAGANY	NIE DOTYCZY		Opisać oferowane parametry
<b>13 OBSŁUGA ROUTINGU</b>					
1)	Obsługa Policy Routingu, routing statyczny i dynamiczny w oparciu o protokoły minimum: RIPv2, OSPF, BGP.	WYMAGANY	NIE DOTYCZY	DT	Opisać oferowane parametry
2)	Możliwość realizacji routingu statycznego w oparciu o polityki automatycznego wyboru łącza w trybie failover.	WYMAGANY	NIE DOTYCZY		Opisać oferowane parametry

3)	Trasowanie pakietów z poziomu wybranej reguły firewall (Policy Based Routing)	WYMAGANY	NIE DOTYCZY		Opisać oferowane parametry
4)	Trasowanie połączeń IPv6 co najmniej w zakresie trasowania statycznego oraz mechanizmu przełączenia na łącze zapasowe w przypadku awarii łącza podstawowego.	WYMAGANY	NIE DOTYCZY		Opisać oferowane parametry
5)	Możliwość agregowania linków fizycznych w oparciu o IEEE 802.3ad (LACP).	WYMAGANY	NIE DOTYCZY		Opisać oferowane parametry
6)	Możliwość wykorzystania mechanizmu SD-WAN poprzez analizę stanu łącza w czasie rzeczywistym i dynamicznym wyborze najkorzystniejszego łącza.	WYMAGANY	NIE DOTYCZY		Opisać oferowane parametry
<b>14 WYDAJNOŚĆ</b>					
1)	Przepustowość Firewall minimum 10 Gbps	WYMAGANY	NIE DOTYCZY	DT	Opisać oferowane parametry
2)	Przepustowość ochrony przed atakami (IPS) minimum 1 Gbps	WYMAGANY	NIE DOTYCZY	DT	Opisać oferowane parametry
3)	Wydajność VPN IPSec minimum 6 Gbps	WYMAGANY	NIE DOTYCZY	DT	Opisać oferowane parametry
4)	Minimalna liczba jednoczesnych połączeń: 1 500 000.	WYMAGANY	NIE DOTYCZY	DT	Opisać oferowane parametry
5)	Minimum 45.000 nowych połączeń na sekundę	WYMAGANY	NIE DOTYCZY	DT	Opisać oferowane parametry
<b>15 BEZPIECZEŃSTWO</b>					
1)	Uwierzytelnianie tożsamości użytkowników za pomocą haseł statycznych i definicji użytkowników przechowywanych w lokalnej bazie systemu.	WYMAGANY	NIE DOTYCZY		Opisać oferowane parametry
2)	Uwierzytelnianie tożsamości użytkowników za pomocą haseł statycznych i definicji użytkowników przechowywanych w bazach zgodnych z LDAP.	WYMAGANY	NIE DOTYCZY		Opisać oferowane parametry
3)	Uwierzytelnianie tożsamości użytkowników za pomocą haseł dynamicznych (RADIUS) w oparciu o zewnętrzne bazy danych.	WYMAGANY	NIE DOTYCZY		Opisać oferowane parametry
4)	Możliwość budowy architektury uwierzytelniania typu Single Sign On w środowisku Active Directory bez konieczności instalowania jakiegokolwiek oprogramowania na kontrolerze domeny.	WYMAGANY	NIE DOTYCZY		Opisać oferowane parametry

5)	Polityka bezpieczeństwa systemu zabezpieczeń musi uwzględniać adresy IP, interfejsy, protokoły, usługi sieciowe, użytkowników, reakcje zabezpieczeń, rejestrowanie zdarzeń oraz zarządzanie pasmem sieci (m.in. pasmo gwarantowane i maksymalne, priorytety).	WYMAGANY	NIE DOTYCZY		Opisać oferowane parametry
<b>16 AKTUALIZACJA</b>					
1)	Automatyczne ściąganie sygnatur ataków, aplikacji, szczepionek antywirusowych oraz ciągły dostęp do globalnej bazy zasilającej filtr URL.	WYMAGANY	NIE DOTYCZY		Opisać oferowane parametry
<b>17 ZARZĄDZANIE</b>					
1)	Elementy systemu muszą zapewniać lokalne zarządzanie (HTTPS, SSH) jak i współpracować z dedykowanymi platformami do centralnego zarządzania i monitorowania.	WYMAGANY	NIE DOTYCZY		Opisać oferowane parametry
2)	Komunikacja systemów zabezpieczeń z platformami zarządzania musi być realizowana z wykorzystaniem szyfrowanych protokołów.	WYMAGANY	NIE DOTYCZY		Opisać oferowane parametry
3)	Interfejs administracyjny musi umożliwiać generowanie skryptów z czynności wykonywanych przez administratora.	WYMAGANY	NIE DOTYCZY		Opisać oferowane parametry
4)	Interfejs administracyjny musi oferować narzędzia do przechwytywania pakietów, wyświetlania otwartych połączeń sieciowych.	WYMAGANY	NIE DOTYCZY		Opisać oferowane parametry
5)	Możliwość eksportowania logów na zewnętrzny serwer (syslog) z wykorzystaniem transmisji nieszyfrowanej jak i szyfrowanej (TLS).	WYMAGANY	NIE DOTYCZY		Opisać oferowane parametry
<b>18 CERTYFIKATY I DEKLARACJE</b>					
1)	Element realizujący zadanie Firewall musi posiadać certyfikat ICSA lub EAL4+ lub równoważny dla rozwiązań kategorii Network Firewall.	WYMAGANY	NIE DOTYCZY		Opisać oferowane certyfikaty i deklaracje
2)	Deklaracja zgodności UE (certyfikat CE) potwierdzająca spełnienie wymagań dyrektywy „Nowego Podejścia”. Urządzenie musi posiadać oznakowanie CE.	WYMAGANY	NIE DOTYCZY		Opisać oferowane certyfikaty i deklaracje





3)	Certyfikat zgodności z dyrektywą RoHS lub dokument wystawiony przez niezależną, akredytowaną jednostkę potwierdzający spełnienie kryteriów środowiskowych zgodnych z dyrektywą RoHS o eliminacji substancji niebezpiecznych.	WYMAGANY	NIE DOTYCZY		Opisać oferowane certyfikaty i deklaracje
4)	Deklaracja zgodności z dyrektywą WEEE lub oświadczenie producenta o spełnieniu obowiązków w zakresie postępowania z odpadami WEEE i zgodności z Ustawą z 11 września 2015 o zużytym sprzęcie elektrycznym i elektronicznym (Dz.U. 2015 poz.1688). Urządzenie musi być oznaczone etykietą WEEE.	WYMAGANY	NIE DOTYCZY		Opisać oferowane certyfikaty i deklaracje
<b>II. Urządzenie UTM dla JO</b>					
<b>1</b>	<b>INFORMACJE OGÓLNE</b>				
1)	Producent/Nazwa rozwiązania/Model	WYMAGANY	NIE DOTYCZY		Podać producenta, nazwę oraz model
<b>2</b>	<b>WYMAGANIA OGÓLNE</b>				
1)	Rozwiązanie musi być dostarczone w postaci komercyjnej platformy sprzętowej z zabezpieczonym systemem operacyjnym.	WYMAGANY	NIE DOTYCZY		Opisać oferowane parametry
2)	Musi być wyposażone w moduł TPM	WYMAGANY	NIE DOTYCZY		Opisać oferowane parametry
3)	Rozwiązanie musi umożliwiać utworzenie kanałów VPN pomiędzy urzędem a Jednostką organizacyjną.	WYMAGANY	NIE DOTYCZY		Opisać oferowane parametry
4)	System ochrony musi realizować funkcjonalności minimum: – poufność danych - IPSec VPN oraz SSL VPN – analiza ruchu szyfrowanego protokołem SSL	WYMAGANY	NIE DOTYCZY		Opisać oferowane parametry
5)	Rozwiązanie musi umożliwiać rozbudowę platformy o funkcjonalność bezpieczeństwa w zakresie (nie wymagane na etapie obecnego postępowania): – kontrola dostępu – zaporą ogniową klasy Stateful Inspection – kontrola stron Internetowych – Web Filter [WF]	WYMAGANY	NIE DOTYCZY		Opisać oferowane parametry

	<ul style="list-style-type: none"> <li>– kontrola zawartości poczty – antyspam [AS] (dla protokołów SMTP, POP3)</li> <li>– kontrola pasma oraz ruchu [QoS i Traffic shaping]</li> <li>– kontrola aplikacji oraz rozpoznawanie ruchu P2P</li> <li>– ochrona przed wirusami – antywirus [AV] (dla protokołów SMTP, POP3, HTTP, FTP, HTTPS). Skanowanie AV dla plików typu: rar, zip;</li> <li>– ochrona przed atakami - Intrusion Prevention System [IPS/IDS]</li> </ul>				
6)	W przypadku potrzeby uruchomienia przez Zamawiającego funkcjonalności bezpieczeństwa jak w pkt 4, rozwiązanie musi spełniać wymagania funkcjonalne i wydajnościowe zgodne z pkt 8-15.	WYMAGANY	NIE DOTYCZY		Opisać oferowane parametry
<b>3 INTERFEJSY</b>					
1)	minimum 8 interfejsów 2,5GbE	WYMAGANY	NIE DOTYCZY	DT	Opisać oferowane parametry
2)	minimum 1 interfejs 1GbE SFP			DT	
<b>4 ZASILANIE</b>					
1)	Zasilacze redundantne o mocy dopasowanej do samodzielnego zapewnienia zasilania urządzenia, pracujące w sieci 230V 50/60Hz.	WYMAGANY	NIE DOTYCZY		Opisać oferowane parametry
<b>5 VPN</b>					
1)	Przepustowość VPN IPSec AES-GCM minimum 2 Gbps			DT	
2)	Tworzenie połączeń w topologii Site-to-site oraz możliwość definiowania połączeń Client-to-site.	WYMAGANY	NIE DOTYCZY	DT	Opisać oferowane parametry
3)	Wsparcie sieci VPN typu, minimum: PPTP VPN, IPSec VPN, SSL VPN	WYMAGANY	NIE DOTYCZY		Opisać oferowane parametry
4)	Klient VPN producenta rozwiązania współpracujący z dostarczonym rozwiązaniem.	WYMAGANY	NIE DOTYCZY		Opisać oferowane parametry
5)	Monitorowanie stanu tuneli VPN i stałego utrzymywania ich aktywności.	WYMAGANY	NIE DOTYCZY		Opisać oferowane parametry
6)	Możliwość przełączania tunelu na łącze zapasowe na wypadek awarii łącza dostawcy podstawowego (VPN Failover)	WYMAGANY	NIE DOTYCZY		Opisać oferowane parametry

7)	Praca w topologii Hub and Spoke oraz Mesh lub równoważnej.	WYMAGANY	NIE DOTYCZY		<i>Opisać oferowane parametry</i>
8)	Obsługa mechanizmów minimum IPSec NAT Traversal, DPD, Xauth.	WYMAGANY	NIE DOTYCZY		<i>Opisać oferowane parametry</i>
9)	Obsługa SSL VPN w trybach portal oraz tunel.	WYMAGANY	NIE DOTYCZY		<i>Opisać oferowane parametry</i>
10)	Obsługa bezpłatnego mechanizmu uwierzytelniania dwuskładnikowego do generowania kodów jednorazowych np. Google Authenticator	WYMAGANY	NIE DOTYCZY	DT	<i>Opisać oferowane parametry</i>
<b>6</b>	<b>BEZPIECZEŃSTWO</b>				
1)	Uwierzytelnianie tożsamości użytkowników za pomocą haseł statycznych i definicji użytkowników przechowywanych w lokalnej bazie systemu.	WYMAGANY	NIE DOTYCZY		<i>Opisać oferowane parametry</i>
2)	Uwierzytelnianie tożsamości użytkowników za pomocą haseł statycznych i definicji użytkowników przechowywanych w bazach zgodnych z LDAP.	WYMAGANY	NIE DOTYCZY		<i>Opisać oferowane parametry</i>
3)	Uwierzytelnianie tożsamości użytkowników za pomocą haseł dynamicznych (RADIUS) w oparciu o zewnętrzne bazy danych.	WYMAGANY	NIE DOTYCZY		<i>Opisać oferowane parametry</i>
4)	Możliwość budowy architektury uwierzytelniania typu Single Sign On w środowisku Active Directory bez konieczności instalowania jakiegokolwiek oprogramowania na kontrolerze domeny.	WYMAGANY	NIE DOTYCZY		<i>Opisać oferowane parametry</i>
5)	Polityka bezpieczeństwa systemu zabezpieczeń musi uwzględniać adresy IP, interfejsy, protokoły, usługi sieciowe, użytkowników, reakcje zabezpieczeń, rejestrowanie zdarzeń oraz zarządzanie pasmem sieci (m.in. pasmo gwarantowane i maksymalne, priorytety).	WYMAGANY	NIE DOTYCZY		<i>Opisać oferowane parametry</i>
<b>7</b>	<b>ZARZĄDZANIE</b>				
1)	Elementy systemu muszą zapewniać lokalne zarządzanie (HTTPS, SSH) jak i współpracować z dedykowanymi platformami do centralnego zarządzania i monitorowania.	WYMAGANY	NIE DOTYCZY		<i>Opisać oferowane parametry</i>



2)	Komunikacja systemów zabezpieczeń z platformami zarządzania musi być realizowana z wykorzystaniem szyfrowanych protokołów.	WYMAGANY	NIE DOTYCZY		Opisać oferowane parametry
3)	Interfejs administracyjny musi umożliwiać generowanie skryptów z czynności wykonywanych przez administratora.	WYMAGANY	NIE DOTYCZY		Opisać oferowane parametry
4)	Interfejs administracyjny musi oferować narzędzia do przechwytywania pakietów, wyświetlania otwartych połączeń sieciowych.	WYMAGANY	NIE DOTYCZY		Opisać oferowane parametry
5)	Możliwość eksportowania logów na zewnętrzny serwer (syslog) z wykorzystaniem transmisji nieszyfrowanej jak i szyfrowanej (TLS).	WYMAGANY	NIE DOTYCZY		Opisać oferowane parametry
<b>8</b>	<b>FIREWALL</b>				
1)	Urządzenie ma być wyposażone w Firewall klasy Stateful Inspection.	WYMAGANY	NIE DOTYCZY		Opisać oferowane parametry
2)	Obsługa translacji NAT oraz PAT.	WYMAGANY	NIE DOTYCZY		Opisać oferowane parametry
3)	Ochrona przed atakami DoS oraz DDoS (flood protection).	WYMAGANY	NIE DOTYCZY		Opisać oferowane parametry
4)	Ochrona przed skanowaniem portów.	WYMAGANY	NIE DOTYCZY		Opisać oferowane parametry
5)	Blokowanie ruchu na podstawie kraju pochodzenia (geolokalizacja IP).	WYMAGANY	NIE DOTYCZY		Opisać oferowane parametry
6)	Filtrowanie na poziomie warstwy 2 modelu OSI tj. na podstawie adresów MAC.	WYMAGANY	NIE DOTYCZY		Opisać oferowane parametry
7)	Możliwość ustawienia trybu pracy jako router warstwy trzeciej, jako bridge warstwy drugiej oraz hybrydowo (częściowo jako router, a częściowo jako bridge).	WYMAGANY	NIE DOTYCZY		Opisać oferowane parametry
8)	Możliwość uwierzytelnienia i autoryzacji użytkowników w oparciu o bazę LDAP, zewnętrzny serwer RADIUS, zewnętrzny serwer Kerberos.	WYMAGANY	NIE DOTYCZY		Opisać oferowane parametry
9)	Musi posiadać wbudowany posiadać wbudowany analizator reguł, który wskazuje błędy i sprzeczności w konfiguracji reguł.	WYMAGANY	NIE DOTYCZY		Opisać oferowane parametry
10)	Możliwość tworzenia wydzielonych stref bezpieczeństwa Firewall np. DMZ.	WYMAGANY	NIE DOTYCZY		Opisać oferowane parametry
<b>9</b>	<b>IPS</b>				



1)	Wykrywanie włamań oraz anomalii w ruchu sieciowym przy pomocy analizy protokołów, analizy heurystycznej oraz analizy w oparciu o sygnatury kontekstowe.	WYMAGANY	NIE DOTYCZY		<i>Opisać oferowane parametry</i>
2)	Usuwanie szkodliwej zawartości w kodzie HTML oraz JavaScript żądanej przez użytkownika strony internetowej bez blokowania dostępu do tej strony po usunięciu zagrożenia	WYMAGANY	NIE DOTYCZY		<i>Opisać oferowane parametry</i>
3)	Wykrywanie anomalii protokołów i ruchu stanowiących podstawową ochronę przed atakami typu DoS oraz DDoS.	WYMAGANY	NIE DOTYCZY		<i>Opisać oferowane parametry</i>
<b>10 ANTYWIRUS</b>					
1)	Silnik antywirusowy musi zapewniać skanowanie ruchu w obu kierunkach komunikacji dla protokołów działających na niestandardowych portach (np. FTP na porcie 2021).	WYMAGANY	NIE DOTYCZY		<i>Opisać oferowane parametry</i>
2)	Możliwość pracy w trybie przezroczystego serwera poczty (Transparent Email Proxy)	WYMAGANY	NIE DOTYCZY		<i>Opisać oferowane parametry</i>
3)	Automatyczna aktualizacja sygnatur zagrożeń.	WYMAGANY	NIE DOTYCZY		<i>Opisać oferowane parametry</i>
4)	Ochrona przed spamem i szkodliwym oprogramowaniem w trakcie transakcji SMTP.	WYMAGANY	NIE DOTYCZY		<i>Opisać oferowane parametry</i>
5)	Inspekcja komunikacji email realizowanej przy użyciu protokołów SMTP, SMTPS, POP3, POP3S.	WYMAGANY	NIE DOTYCZY		<i>Opisać oferowane parametry</i>
6)	Wykrywanie, blokowanie i skanowanie załączników poczty email.	WYMAGANY	NIE DOTYCZY		<i>Opisać oferowane parametry</i>
7)	Tworzenie białych i czarnych list adresów email.	WYMAGANY	NIE DOTYCZY		<i>Opisać oferowane parametry</i>
8)	Wykrywanie spamu niezależnie od stosowanego języka.	WYMAGANY	NIE DOTYCZY		<i>Opisać oferowane parametry</i>
9)	Musi korzystać minimum z dwóch różnych serwerów publikujących listy RBL.	WYMAGANY	NIE DOTYCZY		<i>Opisać oferowane parametry</i>
<b>11 FILTR STRON WWW</b>					

1)	Wbudowany filtr URL oparty o technologię w chmurze z możliwością tworzenia własnych kategorii.	WYMAGANY	NIE DOTYCZY		Opisać oferowane parametry
2)	Filtr URL musi mieć możliwość korzystania z adresów WWW dostępnych w chmurze.	WYMAGANY	NIE DOTYCZY		Opisać oferowane parametry
3)	Musi udostępniać kategorie minimum spam, hacking, malware, botnets.	WYMAGANY	NIE DOTYCZY		Opisać oferowane parametry
4)	Baza filtra WWW musi umożliwiać grupowanie w kategorie tematyczne.	WYMAGANY	NIE DOTYCZY		Opisać oferowane parametry
5)	Filtrowanie treści oraz szkodliwego oprogramowania w obrębie protokołów HTTP i HTTPS.	WYMAGANY	NIE DOTYCZY		Opisać oferowane parametry
6)	Możliwość blokowania i wysyłania treści poprzez HTTP i HTTPS.	WYMAGANY	NIE DOTYCZY		Opisać oferowane parametry
7)	Inspekcja z obsługą protokołu TLS 1.3.	WYMAGANY	NIE DOTYCZY		Opisać oferowane parametry
8)	Filtrowanie plików na podstawie MIME.	WYMAGANY	NIE DOTYCZY		Opisać oferowane parametry
<b>12</b>	<b>KONTROLA APLIKACJI</b>				
1)	Kontrola ruchu na podstawie głębokiej analizy pakietów, nie bazującej jedynie na wartościach portów TCP/UDP.	WYMAGANY	NIE DOTYCZY		Opisać oferowane parametry
2)	Wykrywanie i kontrolę mikroaplikacji (np. Gry portalu Facebook).	WYMAGANY	NIE DOTYCZY		Opisać oferowane parametry
3)	Identyfikacja aplikacji niezależnie od wykorzystywanego portu, protokołu, szyfrowania.	WYMAGANY	NIE DOTYCZY		Opisać oferowane parametry
<b>13</b>	<b>OBSŁUGA ROUTINGU</b>				
1)	Obsługa Policy Routingu, routing statyczny i dynamiczny w oparciu o protokoły minimum: RIPv2, OSPF, BGP.	WYMAGANY	NIE DOTYCZY		Opisać oferowane parametry
2)	Możliwość realizacji routingu statycznego w oparciu o polityki automatycznego wyboru łącza w trybie failover.	WYMAGANY	NIE DOTYCZY		Opisać oferowane parametry
3)	Trasowanie pakietów z poziomu wybranej reguły firewall (Policy Based Routing)	WYMAGANY	NIE DOTYCZY		Opisać oferowane parametry



4)	Trasowanie połączeń IPv6 co najmniej w zakresie trasowania statycznego oraz mechanizmu przełączenia na łącze zapasowe w przypadku awarii łącza podstawowego.	WYMAGANY	NIE DOTYCZY		Opisać oferowane parametry
5)	Możliwość agregowania linków fizycznych w oparciu o IEEE 802.3ad (LACP).	WYMAGANY	NIE DOTYCZY		Opisać oferowane parametry
6)	Możliwość wykorzystania mechanizmu SD-WAN poprzez analizę stanu łącza w czasie rzeczywistym i dynamicznym wyborze najkorzystniejszego łącza.	WYMAGANY	NIE DOTYCZY		Opisać oferowane parametry
<b>14 WYDAJNOŚĆ</b>					
1)	Wydajność systemu Firewall minimum 8 Gbps	WYMAGANY	NIE DOTYCZY		Opisać oferowane parametry
2)	Wydajność ochrony przed atakami (IPS) minimum 4 Gbps	WYMAGANY	NIE DOTYCZY		Opisać oferowane parametry
3)	Minimalna liczba jednoczesnych połączeń: 300.000.	WYMAGANY	NIE DOTYCZY		Opisać oferowane parametry
4)	Minimum 25.000 nowych połączeń na sekundę	WYMAGANY	NIE DOTYCZY		Opisać oferowane parametry
<b>15 AKTUALIZACJA</b>					
1)	Automatyczne ściąganie sygnatur ataków, aplikacji, szczepionek antywirusowych oraz ciągły dostęp do globalnej bazy zasilającej filtr URL.	WYMAGANY	NIE DOTYCZY		Opisać oferowane parametry
<b>16 CERTYFIKATY I DEKLARACJE</b>					
1)	Deklaracja zgodności UE (certyfikat CE) potwierdzająca spełnienie wymagań dyrektywy „Nowego Podejścia”. Urządzenie musi posiadać oznakowanie CE.	WYMAGANY	NIE DOTYCZY		Opisać oferowane certyfikaty i deklaracje
2)	Certyfikat zgodności z dyrektywą RoHS lub dokument wystawiony przez niezależną, akredytowaną jednostkę potwierdzający spełnienie kryteriów środowiskowych zgodnych z dyrektywą RoHS o eliminacji substancji niebezpiecznych.	WYMAGANY	NIE DOTYCZY		Opisać oferowane certyfikaty i deklaracje
3)	Deklaracja zgodności z dyrektywą WEEE lub oświadczenie producenta o spełnieniu obowiązków w zakresie postępowania z odpadami WEEE i zgodności z Ustawą z 11 września 2015 o zużytych sprzęcie elektrycznym	WYMAGANY	NIE DOTYCZY		Opisać oferowane certyfikaty i deklaracje

	i elektronicznym (Dz.U. 2015 poz.1688). Urządzenie musi być oznaczone etykietą WEEE.				
4)	Certyfikat ICSA Labs dla funkcji VPN IPSec lub urządzenie musi znajdować się na liście produktów kryptograficznych zatwierdzonych przez Radę UE	WYMAGANY	NIE DOTYCZY		<i>Opisać oferowane certyfikaty i deklaracje</i>
5)	Certyfikat Common Criteria lub oświadczenie producenta potwierdzające bezpieczeństwo systemu zgodnie z wymaganiami normy ISO 15408.	WYMAGANY	NIE DOTYCZY		<i>Opisać oferowane certyfikaty i deklaracje</i>
6)	Element oferowanego systemu bezpieczeństwa realizujący zadanie Firewall musi posiadać certyfikat ICSA lub EAL4+ lub równoważny dla rozwiązań kategorii Network Firewall.	WYMAGANY	NIE DOTYCZY		<i>Opisać oferowane certyfikaty i deklaracje</i>
<b>III. Wymagania dodatkowe</b>					
<b>1</b>	<b>INSTALACJA I MONTAŻ</b>				
1)	Zamawiający wymaga dostarczenia wszelkich komponentów potrzebnych do zamontowania dostarczonych urządzeń, wniesienia i instalacji urządzeń oraz do połączenia urządzeń do infrastruktury pasywnej (np. szyny montażowe, przewody krosowe RJ45 2m – po 2 sztuki dla każdego dostarczonego urządzenia sieciowego, przewody zasilające, osprzęt montażowy).	WYMAGANY	NIE DOTYCZY		<i>Nie dotyczy*</i>
2)	Wymagana instalacja dostarczonych urządzeń posiadających obudowę przeznaczoną do montażu stelażowego, we wskazanej przez Zamawiającego szafie RACK 19”.	WYMAGANY	NIE DOTYCZY		<i>Nie dotyczy*</i>
3)	Urządzenia muszą być montowane za pośrednictwem szyn montażowych lub uchwytów dostarczonych wraz z urządzeniami.	WYMAGANY	NIE DOTYCZY		<i>Nie dotyczy*</i>
4)	Zamawiający wymaga wykonanie wszystkich połączeń urządzeń, niezbędnych do uruchomienia całości środowiska.	WYMAGANY	NIE DOTYCZY		<i>Nie dotyczy*</i>
<b>2</b>	<b>KONFIGURACJA</b>				





1)	Zamawiający wymaga konfigurację i uruchomienie dostarczonego urządzenia w trybie wysokiej dostępności z istniejącym urządzeniem Fortigate 80F. Po przeprowadzeniu konfiguracji wymagane jest przeprowadzenie testów poprawności działania. Konfiguracja i uruchomienie urządzeń nie może zakłócać i destabilizować pracy urzędu.	WYMAGANY	NIE DOTYCZY	<i>Nie dotyczy*</i>
2)	System UTM dla JO musi zapewniać szyfrowaną wymianę danych z urządzeniem zainstalowanym w Urzędzie. Musi być skonfigurowany zgodnie z wytycznymi administratora Zamawiającego.	WYMAGANY	NIE DOTYCZY	<i>Nie dotyczy*</i>



Fundusze Europejskie  
na Rozwój Cyfrowy



Rzeczpospolita  
Polska

Dofinansowane przez  
Unię Europejską



CENTRUM  
PROJEKTÓW  
POLSKA  
CYFROWA